



(12) **United States Patent**  
**Smith et al.**

(10) **Patent No.:** **US 10,361,849 B2**  
(45) **Date of Patent:** **Jul. 23, 2019**

(54) **METHODS AND SYSTEMS OF PROVIDING VERIFICATION OF THE IDENTITY OF A DIGITAL ENTITY USING A CENTRALIZED OR DISTRIBUTED LEDGER**

(58) **Field of Classification Search**  
CPC ..... H04L 63/061; H04L 63/0435; H04L 63/0823; H04L 63/0442; H04L 9/3247;  
(Continued)

(71) Applicant: **Civic Technologies, Inc.**, Palo Alto, CA (US)

(56) **References Cited**

U.S. PATENT DOCUMENTS

(72) Inventors: **Jonathan Robert Smith**, Oakland, CA (US); **Vinodan Karthikeya Lingham**, Los Altos, CA (US); **John Driscoll**, Fremont, CA (US); **Iain Charles Fraser**, San Francisco, CA (US)

5,818,936 A † 10/1998 Mashayekhi  
9,356,965 B2 † 5/2016 Kjeldas  
(Continued)

OTHER PUBLICATIONS

(73) Assignee: **Civic Technologies, Inc.**, San Francisco, CA (US)

Menezes, A., Katz, J., van Oorschot, P., Vanstone, S., Rosen, K. (1997). Handbook of Applied Cryptography. Boca Raton: CRC Press. pp. 403-405.\*

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(Continued)

*Primary Examiner* — Matthew T Henning

(21) Appl. No.: **15/971,898**

(74) *Attorney, Agent, or Firm* — Foley & Lardner LLP; Daniel Rose

(22) Filed: **May 4, 2018**

(57) **ABSTRACT**

(65) **Prior Publication Data**

US 2018/0255038 A1 Sep. 6, 2018

**Related U.S. Application Data**

(63) Continuation of application No. 15/582,122, filed on Apr. 28, 2017.

(Continued)

(51) **Int. Cl.**  
**H04L 9/32** (2006.01)  
**H04L 9/08** (2006.01)

(Continued)

(52) **U.S. Cl.**  
CPC ..... **H04L 9/0861** (2013.01); **G06Q 20/02** (2013.01); **G06Q 20/065** (2013.01);  
(Continued)

Providing verification of the identity of a digital entity may include including receiving information and a public key of the digital entity, the information having been previously attested to in an attestation transaction stored within a centralized or distributed ledger at an attestation address, the centralized or distributed ledger providing a record of transactions. The system may derive an attestation address using the information and the public key of the digital entity. The system may verify the existence of the attestation transaction at the attestation address in the centralized or distributed ledger and verify that the attestation transaction has not been revoked. The processor associated with the user may receive a cryptographic challenge nonce signed by the digital entity's private key; and may verify the digital entity's identity with the cryptographic challenge nonce signed by the digital entity's key.

**18 Claims, 18 Drawing Sheets**

